

## **Recipe 13 - Configuration Guide for Setting up Sun JES Identity Server 2Q2004 as an AA and CS**

### **Table of Contents**

1	Setup .....	1
1.1	Terms and Introduction .....	1
1.2	Web Server SSL Setup .....	1
2	SAML Server Configuration .....	2
3	Partner Configuration .....	8
3.1	Add an AA .....	9
3.2	Add a CS .....	10
3.3	Setup a Certificate Store .....	11

**Version 2.0.0**

## **1 Setup**

### **1.1 Terms and Introduction**

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and Sun JES Identity Server 2Q2004 as a Credential Service (CS) or as an Agency Application (AA). The Sun setup screens are the same, whether setting up an AA or a CS. In section 2, each type of setup is outlined separately. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the main screen shown in Figure 13-1.

<b>Term</b>	<b>Definition</b>
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

### **1.2 Web Server SSL Setup**

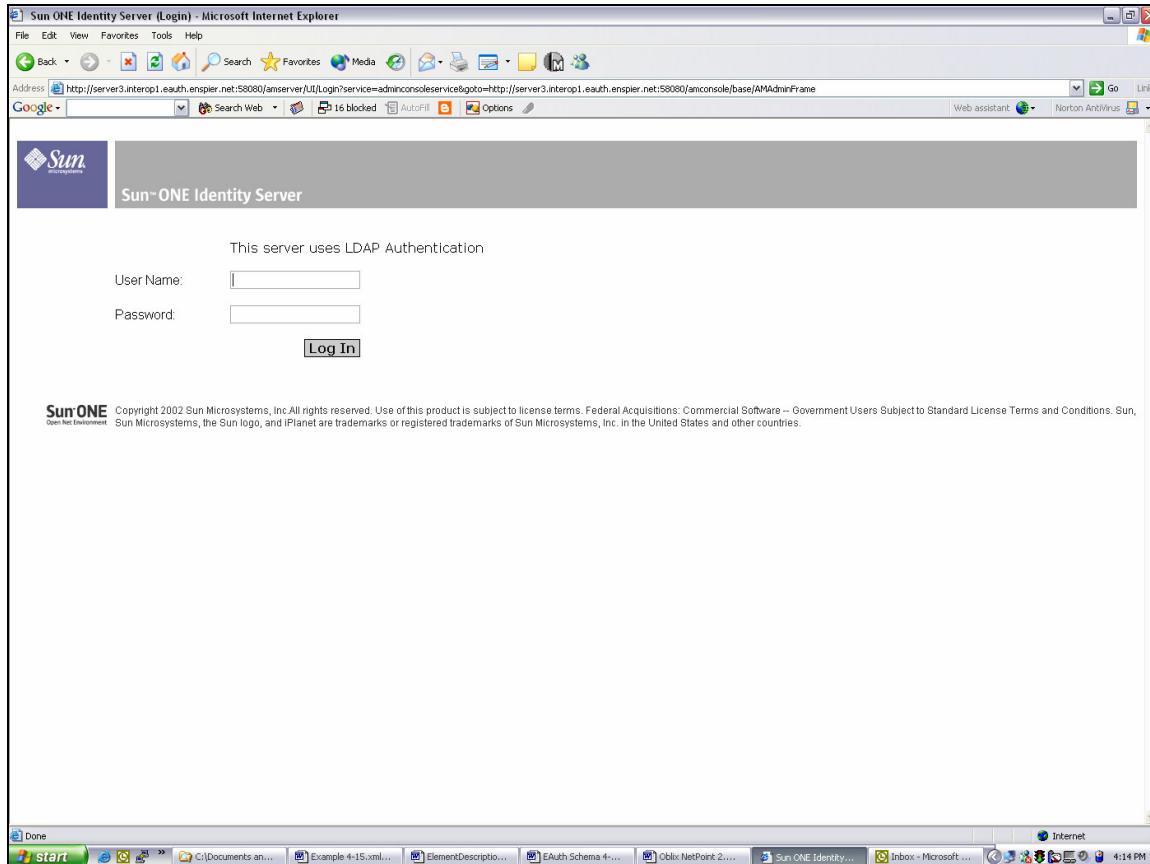
To setup your web server, first enable SSL on the web server that will be running Sun Java System Identity server. Make sure client auth is on. Other than enabling SSL on the web server, you must create a port requiring client certifications.



## 2 SAML Server Configuration

To begin SAML server configuration, you will be logging on to the Sun Java System Identity Server Administration. To access the Sun Java System Identity Server Administration Console, go to:

<http://is.fqdn.com:58080/amconsole>



**Figure 13-1: Security Settings**

After you Login, a screen similar to Figure 13-2 will display. Next, click on the *Service Configuration* tab.

The screenshot shows a Microsoft Internet Explorer window titled "Sun ONE Identity Server - Microsoft Internet Explorer". The address bar contains the URL "http://server3.interop1.eauth.enspier.net:58080/anconsole/base/AMAdminFrame". The top menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar has icons for Back, Forward, Stop, Refresh, Search, Favorites, Media, and others. The status bar shows "Web assistant" and "Norton Antivirus". The main content area has a "Logout" link and a "Welcome amAdmin" message. A navigation bar at the top has tabs for "Identity Management", "Service Configuration" (which is highlighted in yellow), "Current Sessions", and "Federation Management". On the left, there is a search bar labeled "Search" and a sidebar titled "eauth" with a table showing one organization row. The main right panel is titled "eauth" and contains fields for "Full DNS name" (set to "http://server3.interop1.eauth.enspier.net") and "Organization Status" (set to "Active"). It also has sections for "DNS alias names" and "Unique Attribute list". Buttons for "Save" and "Reset" are located at the bottom right of the main panel. A blue callout box with the text "Click on Service Configuration tab" points to the tab in the navigation bar.

**Figure 13-2: Identity Management Page**

Then click the arrow next to *SAML* (under *Service Name*).

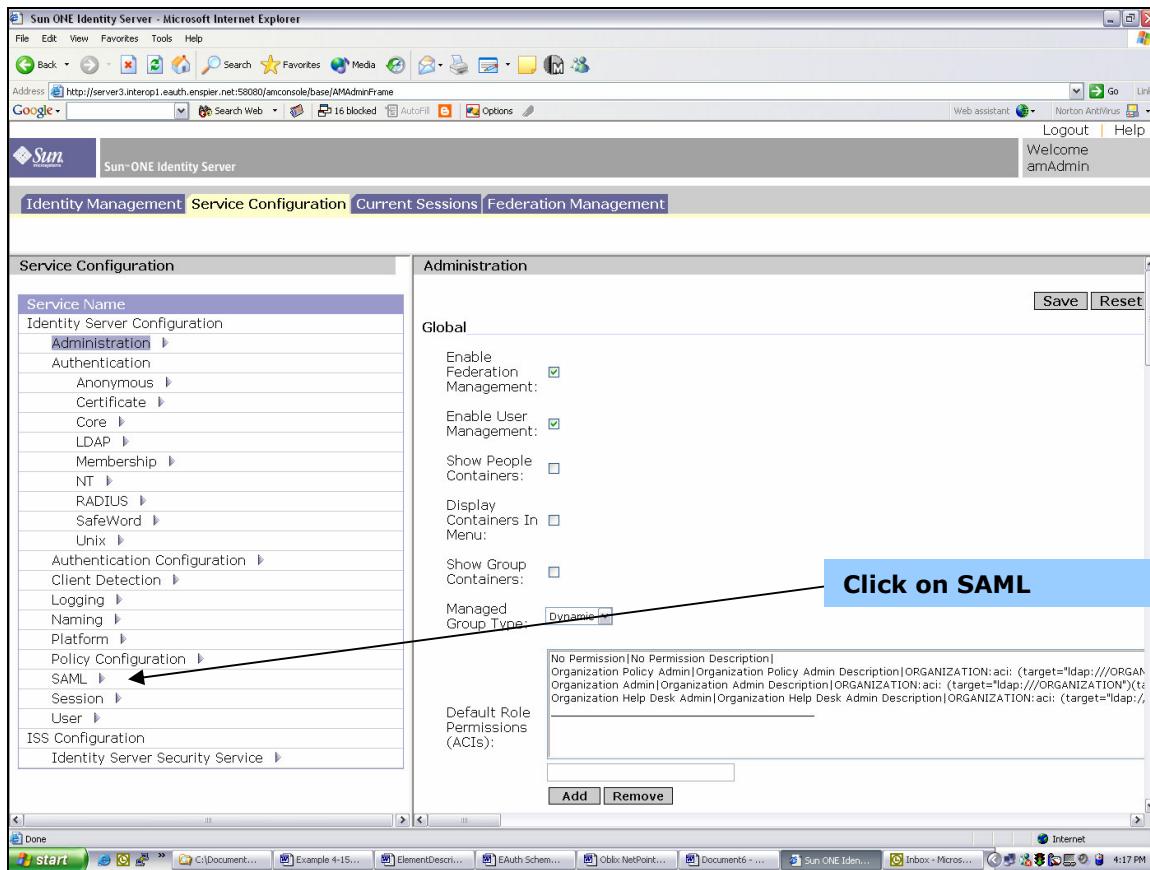
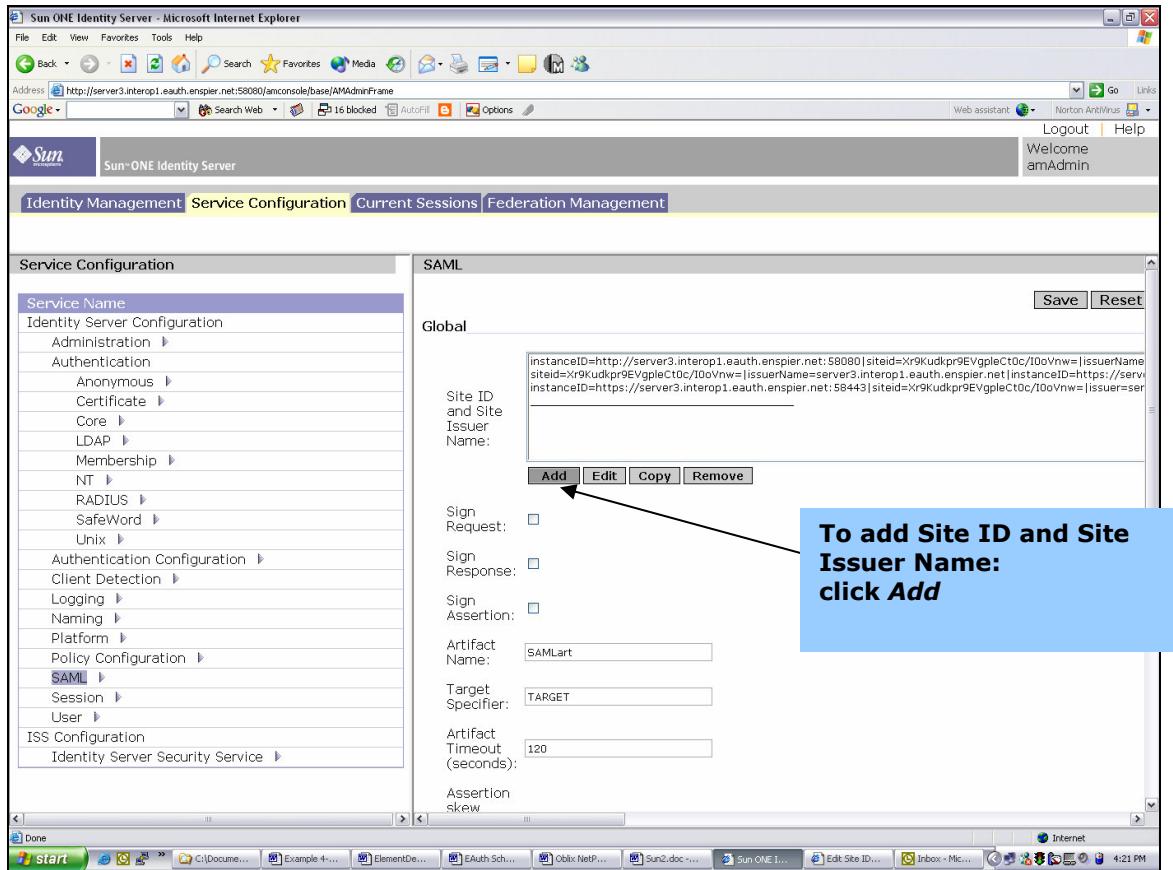


Figure 13-3: Admin Page

When configuring Sun, either as an AA or a CS, you will spend most of your time working with the screen displayed in figure 13-4. Next, click the *Add* button to include a new Site ID and Site Issuer Name.

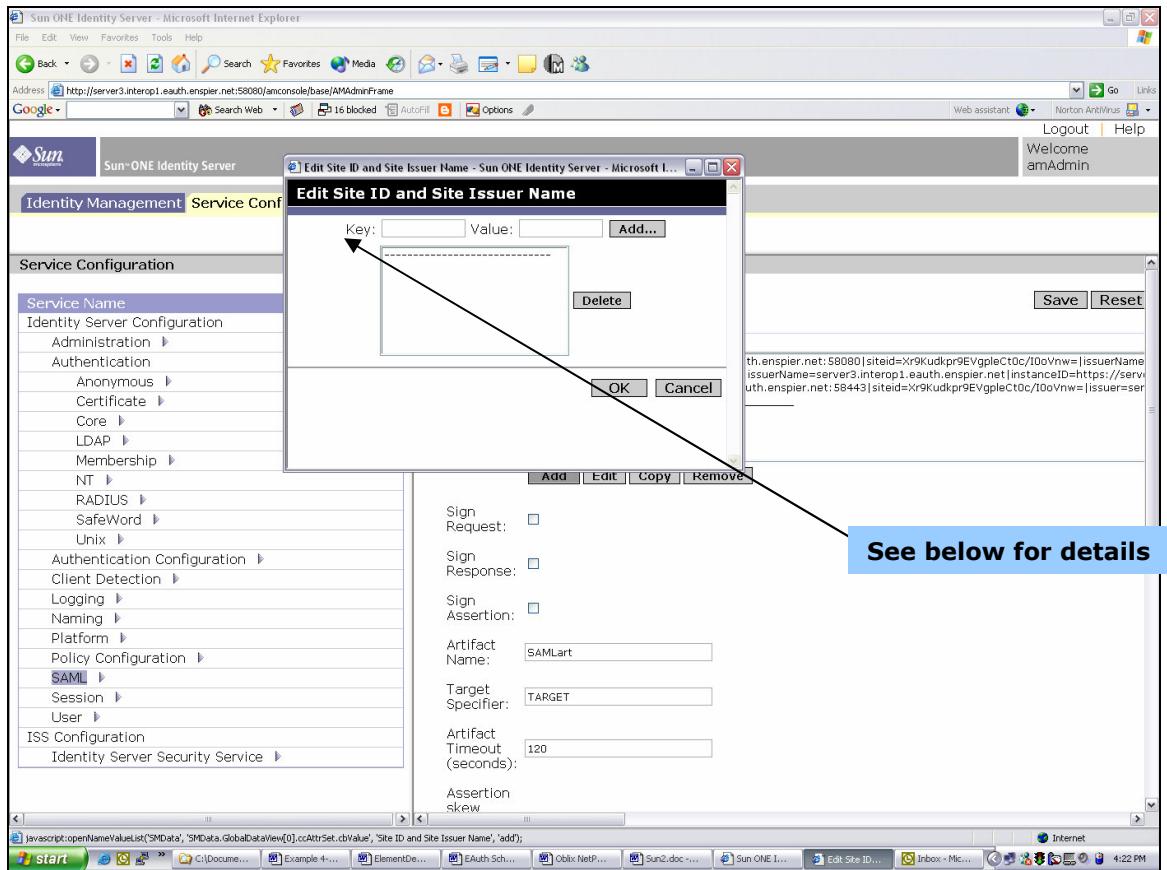


**Figure 13-4: Identity Server Console**

Duplicate the pre-existing Site ID and Site Issuer Name name/value pairs changing only instanceID to reflect the https protocol and the port number. There should be 3 entries in the Site ID and Site Issuer Name section. One for the http port, one for https not requiring a client certificate, and one for https requiring a client certificate.

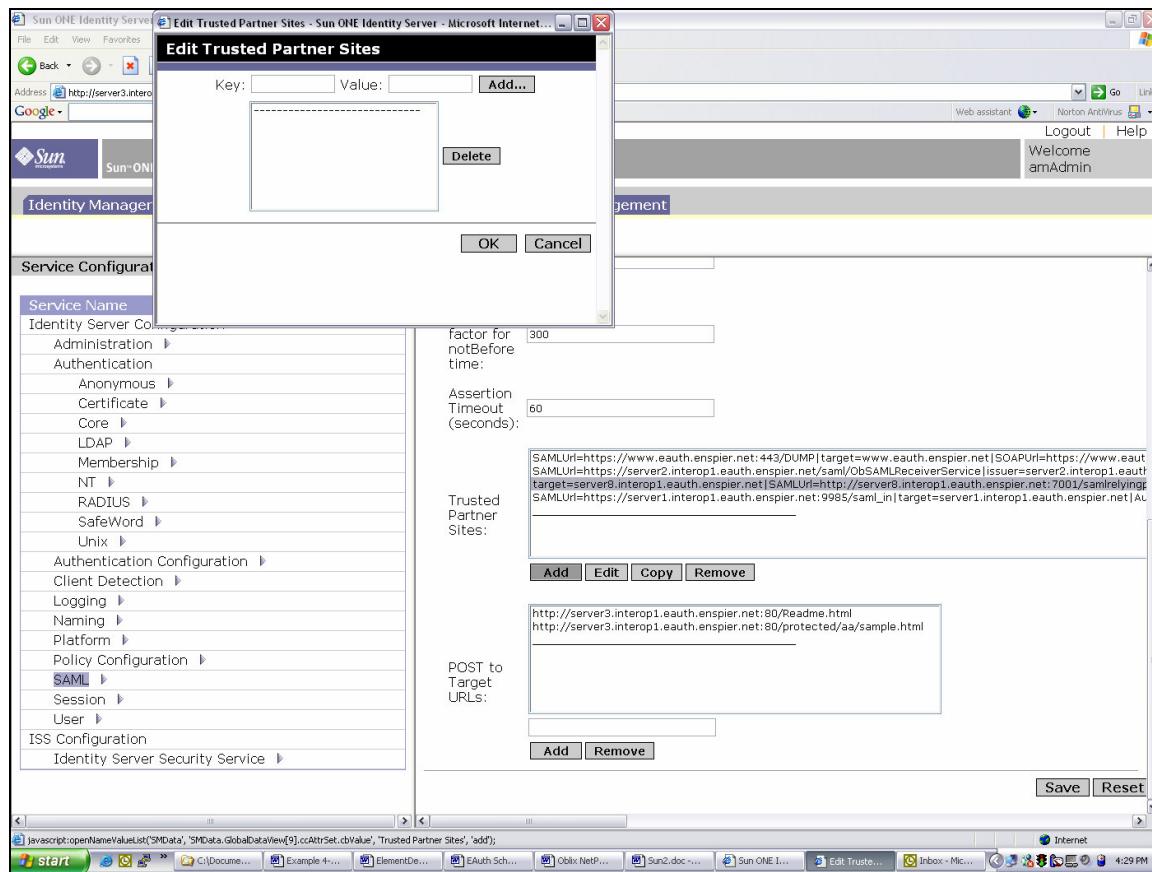
For example:

instanceID=http://is.fqdn.com:58080  
 instanceID=https://is.fqdn.com:58443  
 instanceID=https://is.fqdn.com:58444



**Figure 13-5: Edit Site ID Site Issuer Name**

Next, scroll to the bottom of the page to the “Trusted Partner Sites” section. Click add and the edit screen appears as shown in Figure 13-6.: Fill in different name/value pairs depending upon the role you are configuring (AA or CS).



**Figure 13-6: Edit trusted partner sites**

### 3 Partner Configuration

To add either a CS or an AA, you'll be adding a new line to the Trusted Partner Sites list. You will need to obtain a SourceID for the partner you are adding. Click and select a line under the *Trusted Partner Sites* and then click on *Edit*.

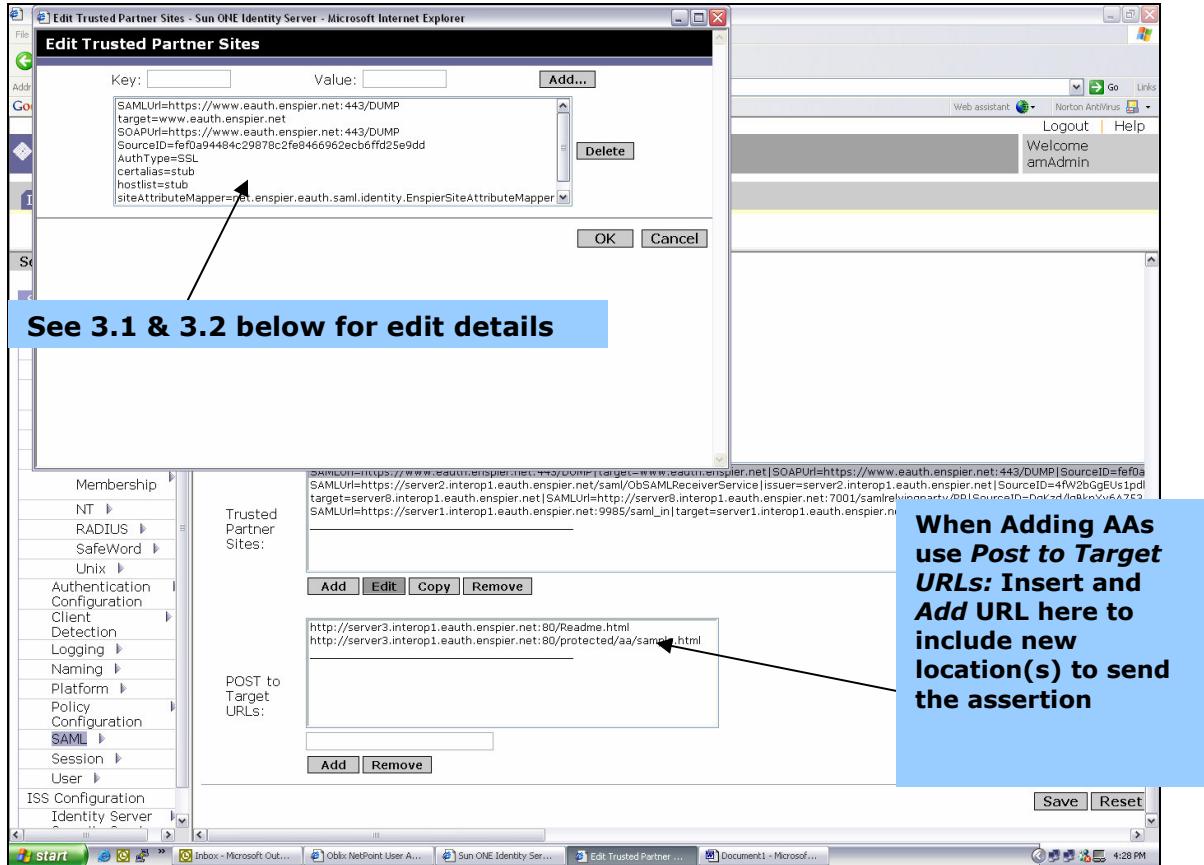


Figure 13-7: Edit trusted partners window

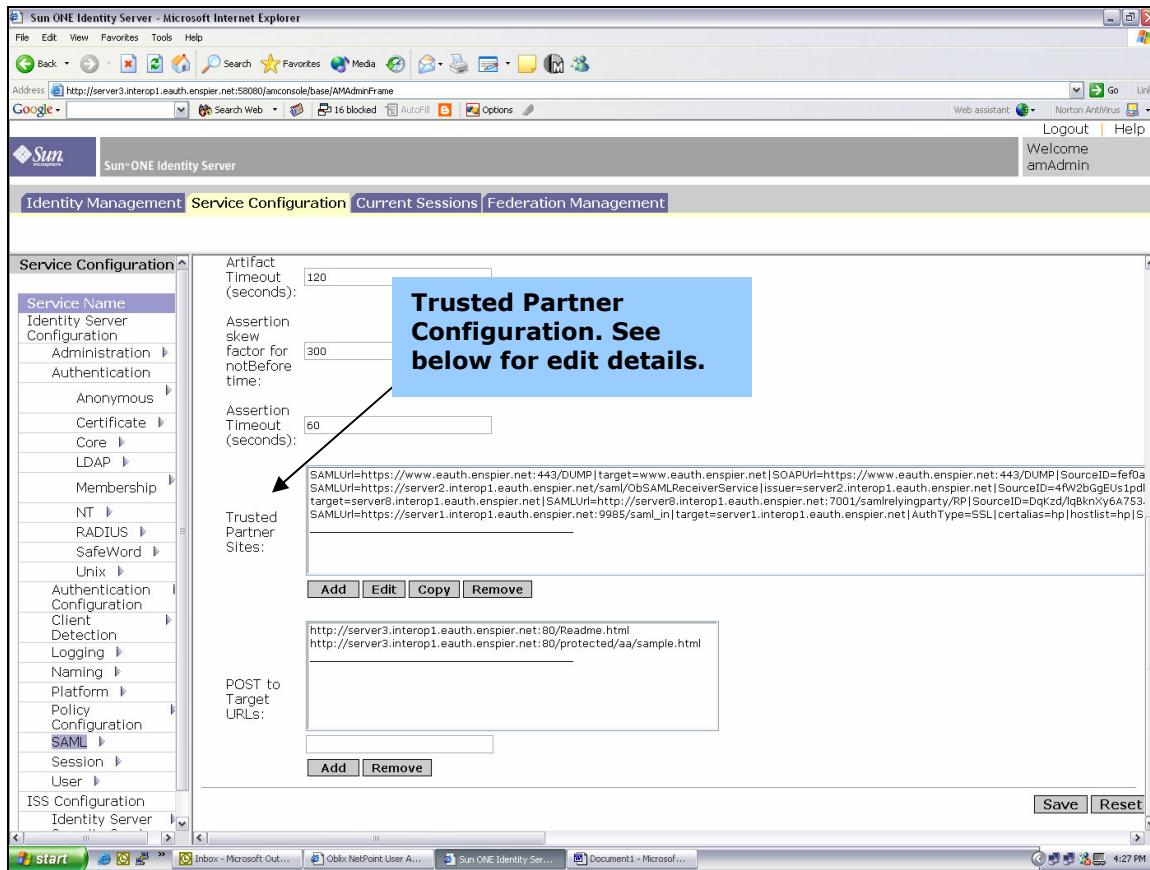
### **3.1 Add an AA**

To add an AA, you must be configured as a CS. Change the following when adding new entry for *Trusted Partner Sites* list:

- Target = fq domain name of partner site
- AuthType = SSL
- Hostlist = cert alias or name (certificate in certificate)
- Site AttributeMapper = java plugin store class to send attribute
- SAML URL = URL of partners artifact receiver

### 3.2 Add a CS

You must be configured as an AA to add a new CS. Edit the list that appears next to the words *Trusted Partner Sites*. Click *Add* when you finish your edits.



**Figure 13-8: Edit Trusted Partner Sites List**

To add a CS you must be configured as an AA. Select a line next to *Trusted Partner Sites*, and click on *Edit*. Change the criteria below, and click on *Add*.

- SOAP URL= URL of SAML responder
- AuthType = SSL
- AttributeMapper = java plugin to read attributes from the assertion
- Action Mapper = java plugin to do things based on the assertion

### 3.3 Setup a Certificate Store

See Solaris and Windows 2000 examples in figure 13-9 for setting up the certificate store.

#### Example 1: Solaris

```
-----  
setenv LD_LIBRARY_PATH /opt/SUNWam/servers/bin/https/lib ( assuming install dir is /opt, change  
it if not to what the install dir is)  
cd /opt/SUNWam/servers/bin/https/admin/bin  
.certutil -A -n greed -t P -d /opt/SUNWam/servers/alias -P https-arth.red.iplanet.com-arth- -f  
/opt/SUNWam/config/.wtpass -i infile
```

Where -d is the com.iplanet.am.admin.cli.certdb.dir parameter from  
/opt/SUNWam/lib/AMConfig.properties  
-P is the com.iplanet.am.admin.cli.certdb.prefix parameter from  
/opt/SUNWam/lib/AMConfig.properties  
-f is the com.iplanet.am.admin.cli.certdb.passfile parameter from  
/opt/SUNWam/lib/AMConfig.properties  
-i is the client certificate of B ( greed).

#### Example 2: Windows2000

```
-----  
assuming product is installed in c:\sunone\sunoneis directory  
go to c:\sunone\sunoneis\server\bin\https\admin\bin  
certutil -A -n greed -t P -d c:\sunone\sunoneis\server\alias -P -P https-arth.red.iplanet.com-arth- -f  
\sunone\sunoneis\config\.wtpass -i infile
```

Where -d is the com.iplanet.am.admin.cli.certdb.dir parameter from  
c:\sunone\sunoneis\lib\AMConfig.properties  
-P is the com.iplanet.am.admin.cli.certdb.prefix parameter from  
c:\sunone\sunoneis\lib\AMConfig.properties  
-f is the com.iplanet.am.admin.cli.certdb.passfile parameter from  
c:\sunone\sunoneis\lib\AMConfig.properties  
-i is the client certificate of B ( greed).

**Figure 13-9: Example Certificate Setup**